

MEMORANDUM OF UNDERSTANDING
BY AND BETWEEN
THE UNITED STATES ARMY CYBER CENTER OF EXCELLENCE (CYBER COE)
AND
THE BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA
BY AND ON BEHALF OF
ARMSTRONG STATE UNIVERSITY
FOR
COLLABORATION IN PROVIDING CYBER TRAINING AND EDUCATION

FTG 16-266

SUBJECT: Training and Education with Cyber CoE and Armstrong University

This Memorandum of Understanding (MOU) between the United States Army Cyber Center of Excellence (USA Cyber CoE) and the Board of Regents of the University System of Georgia, by and on behalf of Armstrong State University (Armstrong) is made and entered into on this second day of June, 2016.

1. BACKGROUND

1.1. As a National Security Agency (NSA) and Department of Homeland Security (DHS) designated National Center of Academic Excellence in Cyber Defense Education (CAE-CD), Armstrong is uniquely qualified and geographically positioned to support the mission needs of the USA Cyber CoE, located at Fort Gordon, GA. Per the NSA/DHS designation, CAE-CDs provide the educational programs needed to prepare students for the workforce to protect the National Information Infrastructure. CAE-CDs must provide depth of education in the following seventeen (17) Knowledge Units (KU):

- Basic Data Analysis
- Basic Scripting
- Cyber Defense
- Cyber Threats
- Databases
- Fundamental Security Design Principles
- Information Assurance (IA) Fundamentals
- Intro to Cryptography
- Information Technology (IT) Systems Components
- Network Defense
- Network Technology and Protocols
- Networking Concepts
- Operating Systems Concepts
- Policy, Legal, Ethics, and Compliance
- Probability and Statistics
- Programming
- Systems Administration

SUBJECT: Training and Education with Cyber CoE and Armstrong State University

1.2. CAE-CDs must have NSA/DHS approved KUs in five (5) additional areas of expertise selected by the institution in accordance with its academic strengths. Armstrong received the NSA/DHS designation as a Center of Academic Excellence for the following five KUs that also directly align with the mission needs of the Cyber CoE:

- IA Compliance
- IA Standards
- Life-Cycle Security
- Operating Systems Theory
- Security Risk Analysis

1.3. Armstrong is a public institution of higher education with over 600 full-time employees and a primary mission to provide excellent academic programs. Armstrong has also been ranked by *Military Times* as being 7th in the nation among four-year schools on its "Best for Vets: Colleges 2016" list. This distinct honor and its proximity to Fort Stewart, Hunter Army Airfield, and Fort Gordon, GA allow Armstrong and the Center for Applied Cyber Education to seamlessly facilitate degree and professional development education and training opportunities for the Cyber CoE.

1.4. The USA Cyber CoE is pursuing a long-term, strategic relationship with Armstrong State University (ASU) to access educational, training, and technical resources in support of the Cyber CoE's mission; to build cyberspace/signal/Electronic Warfare (EW) forces to conduct integrated cyberspace operations and EW; to develop Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) solutions, and to influence the Army's Science and Technology efforts that lead to capabilities that allow the Army to project power in and through cyberspace and the electromagnetic spectrum.

2. Previous Memorandums of Agreement. N/A

3. AUTHORITIES: 10 U.S.C. 2304(c)(3)(B)

4. PURPOSE: This MOU between the Cyber CoE and ASU is for the purpose of fostering a strategic relationship between said parties. The MOU also describes the objectives and scope of ASU-provided education, training and technical support for the Cyber CoE's mission to be Department of Defense's (DoD) recognized experts for cyberspace, signal, and EW, in order to develop DOTMLPF-P solutions that synchronize Warfighting Functions in converging land and cyberspace domains. It establishes the basic assumptions required to enable effective collaboration and support requirements. Each of the undersigned parties understands and agrees to support the objectives and uphold the responsibilities outlined in this MOU.

This MOU is intended to establish a mutually beneficial, cooperative relationship between USA Cyber CoE and Institution for the purposes of:

SUBJECT: Training and Education with Cyber CoE and Armstrong State University

4.1. Developing a nationally recognized Cyber training and mission support capability.

4.2. Delivering education, training, and technical support in cyberspace operations, EW, spectrum management, network transport and information services, network operations, and other areas as determined by the Cyber CoE. Emphasis shall be placed on defensive and offensive cyberspace operations/cyber security, information dominance, information operations, Cyber-EW convergence, and the like.

4.3. Collaborating on and/or co-developing applicable cyberspace capabilities to support Training and Doctrine Command Capabilities Manager-Cyber and the Cyber/Network Battle Lab, as the user representative and experimentation support, respectively, for U.S. Army Cyberspace Command (ARCYBER) Joint Force Headquarters-Cyber, and other Army cyberspace stakeholders (to include corps and below elements).

4.4. Jointly pursuing appropriate training, mission support, and participation in early acquisition insight test/experimentation venues.

4.5. Exploring internships and participation of students/trainees in relevant activities at each institution.

4.6. Developing courseware as needed and directed by the Cyber and Signal Schools for U.S. Army Career Management Fields (CMF) 25 Signal Corps (SC), 29EW, 2210, and the new 17 (Cyber) career fields.

4.7. Developing and executing formalized agreements and contractual documents between the parties, such as an Education Partnership Agreement, Cooperative Research and Development Agreement, Cooperative Agreement, DoD Information Analysis Center Technical Area Task, or similar contractual vehicle to facilitate ASU support to Fort Gordon stakeholders.

5. RESPONSIBILITIES OF THE PARTIES: Specific course offerings and programs will be set forth in the terms of Program Level Agreements (PLAs) between the parties, which will define specific requirements, costs, billing arrangements, and other specifics as required. The Parties here-by agree that they will enter into negotiations for the establishment of PLAs for this purpose. The following responsibilities will be subject to the specific provisions of PLAs, and all regulations and policies applicable to each party's participation in each PLA.

5.1. The Cyber CoE will –

5.1.1. Assist Institution in curriculum development and participate as instructors during seminars and short courses when appropriate.

SUBJECT: Training and Education with Cyber CoE and Armstrong State University

5.1.2. Provide facilities and equipment in support of these educational programs as needed and agreed upon.

5.1.3. Ensure students have the designated security classification for course requirements.

5.1.4. Facilitate internships for degree, non-degree and professional education trainees. Institution's students in certificate, Associate of Science, Bachelor's in Information Technology, Bachelor of Science, and Masters degree programs frequently have co-op and internship opportunities with industry, business, and government.

5.1.5. Collaborate with Institution in order to determine possible solutions for cyberspace operations, EW, and communication networks and information service capability gaps.

5.2. The Institution will –

5.2.1. Develop professional education short courses and facilitate undergraduate/graduate educational opportunities with the degree-granting organizations within the Institution to meet the needs of the Cyber CoE.

5.2.2. Educational offerings may include but will not be limited to:

5.2.2.1. Short Courses: Continuing Education Units from Institution. These do not require admission to the Institution.

Short/continuing education courses are educational programs that offer various options for on-line delivery and feature instructors such as university professors, civilian experts, and current cyber leaders from throughout the DoD. Courses are highly useful from an application point-of-view and will train participants in processes and tools needed to plan, monitor, and improve Cyber Security in their organization. The courses may be conducted at the Institution's main campus in Savannah, Georgia, at the Armstrong Liberty Center campus in Hinesville, Georgia, at Fort Gordon, or at other mutually agreed upon locations.

Specific course content shall be tailored to the needs of the Cyber CoE. For example, current Institution credit-bearing course content can be leveraged for formal and informal training and would be complimentary to the current Joint Cyber Analysis Course courseware with the added dimension of Institution faculty, who support cutting-edge DoD-funded cyber projects, conducting the bulk of the instruction or augmenting the instruction of DoD cyber security professionals. Upon completion of each continuing education course, students will receive an Institution certificate for the course taken.

SUBJECT: Training and Education with Cyber CoE and Armstrong State University

By way of example, and not limitation, short/continuing education courses tailored from existing ASU credit bearing courses may include:

- Cyber Security: A Systems Approach
- Mobile Device Security
- Network Security
- Exploitation and Defense of IT Systems: Hands on Lab
- Cyber Security of Embedded Systems
- Cyber Test and Evaluation
- Penetration Testing
- Incident Response
- Secure Software Development and Design
- Identification and Access Management
- Digital Forensics
- Device Forensics
- Host Forensics

5.2.2.2. Degree Programs: Each of the following degree programs requires admission to the Institution:

From the Department of Computer Science and IT:

Bachelor's in IT, Cyber Security Track – designed for students seeking a four-year Bachelor's of Science degree, this curriculum includes the university's core curriculum, as well as advanced courses in information technology and cyber security. (This degree meets all of the requirements [knowledge units] for the NSA/DHS Center of Academic Excellence program).

Undergraduate Certificate in Cyber Security – designed for students who do not intend to earn (another) college degree, but want to obtain certification in the growing cyber security field. It requires prerequisite math and Information Technology courses as well as three cyber security courses. Seven courses total (six if the Math pre-requisite has been fulfilled).

Associate of Science, Cyber Security Track – designed for students seeking a two-year Associate of Science Degree, this curriculum includes the university's core curriculum, as well as prerequisite IT courses and three cyber security courses. This track may also be a stepping-stone toward the Bachelor's of IT Degree.

Health Informatics track for a Master of Science in Computer and Information Science Degree – A masters level program designed to safeguard patients' health care information. From the Department of Criminal Justice, Social and Political Science:

SUBJECT: Training and Education with Cyber CoE and Armstrong State University

Minor in Cyber Crime – designed for students who are already enrolled in a baccalaureate degree program who are interested in obtaining a concentration in cyber forensics/cyber crime.

Bachelor of Science with a major in Criminal Justice, Cyber Crime track - designed for students who want an interdisciplinary degree that prepares them for the demands of the market place. Its graduates have been successful in garnering well paying jobs in cyber crime and cyber forensics.

Graduate Certificate in Cyber Crime - This post-baccalaureate certificate builds on students' baccalaureate degrees and may also serve as a stepping-stone toward the Master of Science in Criminal Justice Degree. Fully online program.

Interdisciplinary Minor in Cyber Security – designed for students who are already enrolled in a baccalaureate degree program. In addition to basic Information Technology courses, it requires three courses in cyber security and one course in cyber crime.

Non-Degree, Special Status students: It is possible for students to be admitted as non-degree students and register for classes on-campus or online. These students participate with other students in classes and get an Institution transcript with letter.

5.2.3. Facilitate internships for the professional educator.

5.2.4. Conduct boot camp courses for personnel needing preparatory classes before joining degree programs.

5.2.5. Brief and initiate the evaluation/enrollment process for new students prior and during all new Cyber training start-up sessions.

5.2.6. During Cyber student Graduation ceremonies, the Institution shall be on hand to present an official institutional certificate of training and possible transcripts containing the regional awarded college credit for the dual enrolled courses and/or residential on-line institutional required courses.

5.3. To meet the objectives described above, both Parties agree to:

5.3.1. Assign Curriculum Development Coordinators (each party) for implementation of the Educational Development part of this MOU.

5.3.2. Create an accredited articulated cooperative (program) covering Cyber degrees and certificates of training.

5.3.3. Investigate ways for non-degree seeking students to enroll in credit courses.

SUBJECT: Training and Education with Cyber CoE and Armstrong State University

5.3.4. Develop courseware as needed and directed by the Cyber and Signal Schools for CMFs 25 (SC), 29 (EW), 2210, and 17 (Cyber) career fields (which may include non-classified and classified material).

5.3.5. Explore the sponsoring of an annual cyber security training event (e.g., workshop, exercise, conference, etc.).

5.3.6. Establish quarterly meetings (alternating between locations or by conference/teleconference/video teleconference/online participation if agreeable to both parties). The intent is to provide representatives from all organizations the opportunity for ongoing information sharing regarding current, planned, and/or new initiatives and activities.

5.3.7. Meet annually to review activities of the past year, and plans for the following year.

5.3.8. An on-line co-enrollment with the Institution when Service members are assigned to Fort Gordon for formal Cyber and/or Signals training.

5.3.9. Adhere to each party's respective security rules and regulations when courses, meetings and conferences are hosted at Cyber CoE and the Institution.

6. PERSONNEL: Each Party is responsible for all of its personnel costs including pay and benefits, support, and travel. Each Party is responsible for supervision and management of its personnel. There will be no shared responsibility for management and/or supervision of personnel.

7. GENERAL PROVISIONS:

7.1. POINTS OF CONTACT: The Parties will use the following Points of Contact (POC) in the implementation of this MOU. Each Party may change its POC upon reasonable notice to the other Party, and may appoint alternate POCs as needed.

7.1.1. For the Cyber CoE–

Primary POC: Ms. Gloria Palmer, G-8, (706) 791-8753,
gloria.m.palmer2.civ@mail.mil.

7.1.2. For the Institution–

Primary POC: Mr. Scott Scheidt, Director of the Center for Applied Cyber Education, (912) 344-3330, scott.scheidt@armstrong.edu.

SUBJECT: Training and Education with Cyber CoE and Armstrong State University

7.2. CORRESPONDENCE: The Parties will address all written correspondence sent or received specific to the content of this MOU as follows, unless directed otherwise:

7.2.1. For the Cyber CoE -

Department of the Army
U.S. Army Cyber Center of Excellence (Cyber CoE)
ATTN: ATZH-DT
506 Chamberlain Ave
Bldg 29808, Room 507
Fort Gordon, GA 30905

7.2.2. For Armstrong -

Armstrong State University
ATTN: Director, Center for Applied Cyber Education
College of Science and Technology
11935 Abercorn Street
Savannah, GA 31419

7.3. MODIFICATION: This MOU may only be modified by the written agreement of the Parties, duly signed by their authorized representatives. Such amendments will be dated, consecutively numbered, and appended to each copy of this document.

7.4. EXPIRATION: This MOU expires nine years and one day after the signature of the last Party. If the agreement is to remain in effect after the nine-year period, it can be re-signed in conjunction with the third triennial review.

7.5. TERMINATION: Either party may unilaterally terminate the agreement prior to the expiration date on 180 days notice. If there are no PLAs in place and there are no outstanding issues involving reimbursement, this MOU may be unilaterally terminated by either party prior to the expiration date by providing 30 days of advance notification. The MOU may also be terminated at any time upon the mutual written consent of the Parties.

7.6. NO TRANSFER: This MOU is not transferable except with the written consent of the Parties.

7.7. ENTIRE UNDERSTANDING: It is expressly understood and agreed that with the exception of any PLAs developed in accordance with this MOU, this MOU embodies the entire agreement between the Parties regarding the MOU's subject matter.

7.8. EFFECTIVE DATE: This MOU takes effect beginning on the day and date written above.

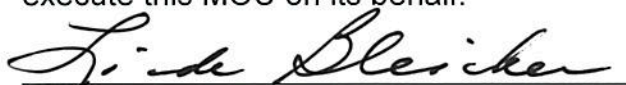
8. FINANCIAL DETAILS:

8.1. AVAILABILITY OF FUNDS: This MOU does not document the obligation of funds between the Parties. Any obligation of funds in support of this MOU will be accomplished as mutually agreed to by both Parties. The obligation of the funds by the Parties is subject to the availability of appropriated funds pursuant to the DoD Financial Management Regulation and the availability of funds appropriated and allocated to Armstrong, as determined in Armstrong's sole discretion.

8.2. BILLING: The institution will bill the lead organizations, as designated by the Cyber CoE, in accordance with the procedures established for products and/or services in the applicable PLA or as otherwise agreed upon by supplemental negotiation between the Parties. The Parties will maintain a record of the transactions by written/electronic correspondence between the Parties or by annual report after the month in which the first transaction occurred. Billing will be established in the applicable PLA or as otherwise agreed to by the Parties. Reimbursement will occur as mutually negotiated within the structure of the individual PLAs.

8.3. FINANCIAL SPECIFICS: See the applicable PLAs established in regard to agreed upon products and services or other supplemental agreements for details and information on the reimbursable support identified pursuant to the responsibilities identified in this MOU.

In witness whereof, each of the parties have caused its authorized representative to execute this MOU on its behalf.



LINDA BLEICKEN
President, Armstrong State University



STEPHEN G. FOGARTY
Major General, U.S. Army
U.S. Army CYBER Center of Excellence

Approved as to form
Armstrong State University
Office of Legal Affairs
E. Lee Davis, University Counsel
2016.06.01